Name: Deep Pawar
CWID: A20545137
Sub: CS536 SOP Assignment 4

Date
Page

Q. 1.

a) $p[y+z/x]$

→

$p[y+z/x] \equiv (w \cdot x \neq 0 \wedge z \leq 2 \rightarrow f(w) > 0$
$\wedge \forall x . \exists y . 0 \leq y \leq x \wedge f(w \div x) + y > f(z))$

$p[y+z/x]$
$\equiv (w * e \neq 0 \wedge z \leq 2) \rightarrow (f(w) > 0 \wedge$
$\forall x . \exists y . 0 \leq y \leq x \wedge f(w \div x) + y > f(z)$

$p[y+z/x]$
$\equiv w * (y+z) \neq 0 \wedge z \leq 2 \rightarrow f(w) > 0$
$\wedge \forall x . \exists y . 0 \leq y \leq x \wedge f(w \div x) + y > f(z)$

b) $p[x+z/w]$

→

$p[x+z/w]$
$\equiv ((x+z) \cdot x \neq 0 \wedge z \leq 2 \rightarrow f(x+z) >$
$0 \wedge \forall x_0 . \exists y . 0 \leq y \leq x_0 \wedge f((x+z) \div x_0)$
$+ y > f(z))$

$p[x+z/w]$
$\equiv ((x+z) \cdot x \neq 0 \wedge z \leq 2 \rightarrow f(x+z) >$
$0 \wedge \forall x_0 . \exists y . 0 \leq y \leq x_0 \wedge f(x+z) \div x_0)$
$+ y > f(z))$

c) $p[x+y/z]$

→

$p[x+y/z]$
$\equiv (w \cdot x \neq 0 \wedge (x+y) \leq 2 \rightarrow f(w) > 0$
$\wedge \forall x_0 . \exists y_0 . 0 \leq y_0 \leq x_0 \wedge f(w \div x_0) +$
$y_0 > f(x+y))$

Date
Page

Q. 2 Let x & y be two different integer variables.

$$(x * y)[e/x][e'/y] \equiv (x * y)[e'/y][e/x]$$

a) Show an example in which the above conjecture works

→ Let,

$e = 4$ and $e' = 2$

L.H.S,

$$(x * y)[4/x][2/y] = (4 * y)[2/y]$$
$$= 4 * 2$$
$$= 8$$

R.H.S.

$$(x * y)[2/y][4/x] = (x * 2)[4/x]$$
$$= 4 * 2$$
$$= 8$$

$\boxed{\therefore \text{LHS} = \text{RHS}}$

b) Disaprove the above conjecture with a counterexample

→ Let,

$e = y$ and $e' = x$

L.H.S,

$$(x * y)[y/x][x/y] = y * y[x/y]$$
$$= x * x$$

R.H.S.

$$(x * y)[x/y][y/x] = x * x[y/x]$$
$$= y * y$$

$\boxed{\therefore \text{LHS} \neq \text{RHS}}$

Therefore, this disaproves the conjecture

Q 3.

a) Prove that "If $p \Leftrightarrow wlp(S, q)$ then $sp(p, S) \Rightarrow q$"

→ Here,

$p \Leftrightarrow wlp(S, q)$ implies that $\models \{p\}\ S\ \{q\}$

... by definition of weakest liberal precondition

$\models \{wlp(S, q)\}\ S\ \{q\}$

... weakening the precondition

Let τ be a state such that $\tau \models sp(p, S)$

By the definition of $sp(p, S)$ there exists some $\sigma \models p$ such that $\tau \in M(S, \sigma) - \bot$

$\models \{p\}\ S\ \{q\}$ implies that $M(S, \sigma) - \bot \models q$

thus $\tau \models q$.

Thus, if $\tau \models sp(p, S)$, then $\tau \models q$ which implies $sp(p, S) \Rightarrow q$. Hence proved.

b) Disprove that "if $p \Leftrightarrow wlp(S, q)$ then $q \Rightarrow sp(p, S)$"

→ Here,

$p \Leftrightarrow wlp(S, q)$ implies that $\models \{p\}\ S\ \{q\}$

... by definition of weakest liberal precondition

$\models \{wlp(S, q)\}\ S\ \{q\}$

... weakening the precondition

By the definition of $sp(p, S)$, we have $\models \{p\}\ S\ \{sp(p, S)\}$.

Since $sp(p, S) \Rightarrow q$, it implies that a triple may or may not hold true if post condition is weakened. It contradicts the claim that $sp(p, S)$ is stronger than q.

Counterexample can be,

if $S \equiv x := x * x$ and $q \equiv x < 1$

then $wlp(S, q) \equiv x * x < 1 \Leftrightarrow x = 0$.

But $sp(x = 0,\ x := x * x) \equiv (x_0 = 0 \wedge x = x_0 * x_0)$

$\Rightarrow x = 0$, which is strictly stronger than $x < 1$.

Hence, the above statement cannot be true

Date
Page

Q. 4.

a) $\models_{tot} \{p\}\ S\ \{s\}$
→ $\boxed{\text{False}}$

Explanation:
Here,
$$s \iff sp(p, S)$$
i.e. $\models \{p\}\ S\ \{s\}$
But it is possible that
$$\exists \tau = \perp \in M(S, \sigma)$$
Hence, it does not satisfy triple under total correctness

b) There exists some $\sigma \models p$ such that $\sigma \not\models \{p\}\ S\ \{q\}$
→ $\boxed{\text{False}}$

Explanation:
If a state is satisfying pre-condition & s is logically equivalent to $sp(p, S)$ can satisfy the pre-condition & may not satisfy the strongest postcondition. It can either diverge or create errors on S.
i.e. if $\sigma \models p$ then $M(S, \sigma) - \perp \models s$

c) For each state $\sigma \models p$, we have that $M(S, \sigma) \models s$
→ $\boxed{\text{False}}$

Explanation:
If $\sigma \models p$ then $\forall \tau \in M(S, \sigma) \cdot \tau = \perp \vee \tau \models s$.
Which means it either leads to pseudo-states or satisfies the strongest post condition.

d) If $M(S, \sigma) \neq \perp \models s$, then $\sigma \models p$

→ $\boxed{\text{False}}$

Explanation:

Knowing that S terminates & that s holds upon termination does not guarantee that the precondition p was initially true. s could hold as a result of conditions or assignments within S, even if p did not hold before execution. i.e. just because S terminates & s holds afterward does not imply that the initial condition ~~i~~ p was true.

e) If $\sigma \models \neg p$ then $\sigma \models \{\neg p\}\ S\ \{\neg s\}$ ~~{q}~~ :

→ $\boxed{\text{False}}$

Explanation:

If $\sigma \models \neg p$ i.e. $\sigma \not\models p$ then we don't know anything interesting between $M(S, \sigma)$ & strongest postcondition $sp(p, S)$.

Date
Page

Q. 5 Calculate $sp(x = y,\ \text{if } x \geq 0 \rightarrow x := y + 1;\ z := x \ \Box\ x \leq 0 \rightarrow y := x - 1;\ z := y \text{ fi})$

→ Let

$IF \equiv \text{if } x \geq 0 \rightarrow x := y + 1;\ z := x \ \Box\ x \leq 0 \rightarrow y := x - 1;\ z := y \text{ fi}$

$sp(x = y, IF)$

$\equiv sp(x = y \wedge x = x_0 \wedge y = y_0 \wedge x \geq 0,\ x := y + 1;\ z := x) \vee sp(x = y \wedge x = x_0 \wedge y = y_0 \wedge x \leq 0,\ y := x - 1;\ z := y)$

$\equiv sp(x_0 = y \wedge x_0 = x_0 \wedge y = y_0 \wedge x_0 \geq 0 \wedge x = y + 1,\ z := x) \vee sp(x = y_0 \wedge x = x_0 \wedge y_0 = y_0 \wedge x \leq 0 \wedge y = x - 1,\ z := y)$

$\equiv (x_0 = y \wedge x_0 = x_0 \wedge y = y_0 \wedge x_0 \geq 0 \wedge x = y + 1 \wedge z = x) \vee (x = y_0 \wedge x = x_0 \wedge y_0 = y_0 \wedge x \leq 0 \wedge y = x - 1 \wedge z = y)$

Q. 6 Calculate $sp(y = x + 1,\ y := y + 1;\ \text{if } x < 0 \text{ then } y := -y \text{ fi})$

→ Here,

$y = x + 1$ ... ①

and

$y := y + 1$

$\therefore y = x + 1 + 1$ ... from ①

$\therefore y = x + 2$

Now, lets calculate conditional statement :

$\text{if } x < 0 \text{ then } y := -y \text{ fi}$

$\therefore y = -(x + 2)$

$= -x - 2$ ... if $x < 0$

for false statement i.e.

if $x \geq 0$ then $y = x + 2$

So,

the strongest postcondition $sp(y = x + 1, y := y + 1;$ if $x < 0$ then $y := -y$ fi $)$ is therefore

$\Leftrightarrow (x < 0 \wedge y = -x - 2) \vee (x \geq 0 \wedge y = x + 2)$

$$\boxed{\therefore\ y = \begin{cases} x + 2, & \text{if } x \geq 0 \\ -x - 2, & \text{if } x < 0 \end{cases}}$$

Q. 7.

→ For formal proof:

$\{p \wedge B\}\ S_1\ \{q_1\}$ and $\{p \wedge \neg B\}\ S_2\ \{q_2\}$

To prove:

$\vdash \{p\}$ if B then S_1 else S_2 fi $\{q_1 \vee q_2\}$

Proof:

① $\{p \wedge B\}\ S_1\ \{q_1\}$ --- given

② $\{p \wedge \neg B\}\ S_2\ \{q_2\}$ --- given

③ $\{p \wedge B\}\ S_1\ \{q_1 \vee q_2\}$ ... Consequence rule

④ $\{p \wedge \neg B\}\ S_2\ \{q_1 \vee q_2\}$ ... Consequence rule

⑤ $(B \rightarrow (p \wedge B)) \wedge (\neg B \rightarrow (p \wedge \neg B)) \Leftrightarrow p$ ... Logical equivalence

⑥ $\{(B \rightarrow (p \wedge B)) \wedge (\neg B \rightarrow (p \wedge \neg B))\}$ if B then S_1 else S_2 fi $\{q_1 \vee q_2\}$ --- By conditional rule 2 using steps ③ & ④

⑦ $\{p\}$ if B then S_1 else S_2 fi $\{q_1 \vee q_2\}$ --- By consequence rule using steps ⑤ & ⑥

$\therefore$ Hence proved.

Date ________
Page ________

Q. 8.

→ Given,

$S \equiv x := x * x \; ; \; y := 2 * y$

step ① : Calculate $wlp(S, x = y)$

For $y := 2 * y$

∴ Before this $x = 2 * y$ must hold

For $x := x * x$

∴ Before this $x * x = 2 * y$ must hold

∴ $wlp(S, x = y) \iff x * x = 2 * y$

step ② : Proof $\vdash \{p\} \; S \; \{x = y\}$

Given,

$p \equiv wlp(S, x = y)$

we have,

$p \equiv \{x * x = 2 * y)$

we need to prove $\vdash \{p\} \; S \; \{x = y\}$

i) Precondition : $p \equiv (x * x = 2 * y)$

ii) Sequence of statements :

$x := x * x$

$y := 2 * y$

iii) Show that executing $x := x * x$ preserves p :

Since,

$x * x = 2 * y$, the intermediate condition $x = 2 * y$ will hold after this step.

iv) show that executing $y := 2 * y$ establishes the postcondition $x = y$:

After $y := 2 * y$, y takes the value $2 * y$

Since $x = 2 * y$ held after first assignment $x = y$ now holds.

Thus, ~~proved that~~

$\vdash \{x * x = 2 * y\} \; S \; \{x = y\}$

Hence proved.

Q. 9.

→ Rules for $R_1 \rightarrow R_5$:

R_1 : Forward assignment
R_2 : Forward assignment
R_3 : Sequence rule 1, 2
R_4 : Weakening Postcondition 3, 4
R_5 : ~~while~~ ~~loop~~ ~~rule~~ loop 5

Q. 10.

→ Rules for R_1 to R_{11} :

R_1 : Forward assignment
R_2 : Forward assignment ; no aging se
R_3 : weakening post condition 2, 3
R_4 : Sequence rule 1, 4
R_5 : Backward assignment
R_6 : Backward assignment
R_7 : Stregthning precondition 8, 7
R_8 : Sequence rule 9, 6
R_9 : loop 10
R_{10} : Sequence rule 5, 11
R_{11} : weakening postcondition 12, 13